

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 1 日
Date of Application:

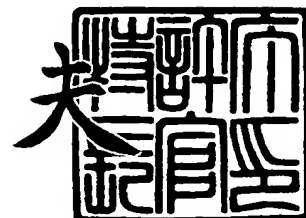
出 願 番 号 特 願 2 0 0 2 - 2 9 9 7 2 1
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 9 9 7 2 1]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 8 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0206874

【提出日】 平成14年10月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00 537

【発明の名称】 電子ファイル管理装置

【請求項の数】 7

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社リコー内

【氏名】 斉藤 敦久

【特許出願人】

【識別番号】 000006747

【氏名又は名称】 株式会社リコー

【代表者】 桜井 正光

【代理人】

【識別番号】 100084250

【弁理士】

【氏名又は名称】 丸山 隆夫

【電話番号】 03-3590-8902

【手数料の表示】

【予納台帳番号】 007250

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0207936

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 電子ファイル管理装置

【特許請求の範囲】

【請求項1】 データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから生成されたアクセス制限電子ファイルとを、当該オリジナル電子ファイルに対するアクセス権限情報に基づいて管理することを特徴とする電子ファイル管理装置。

【請求項2】 データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから前記アクセス制限手段により生成されたアクセス制限電子ファイルとを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリ



ジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項 3】 データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルから前記アクセス制限手段によりアクセス制限電子ファイルが生成されると、該オリジナル電子ファイルを破棄して生成されたアクセス制限電子ファイルを前記格納手段に格納し、アクセス要求を受けると、アクセス制限電子ファイルを前記格納手段から出力することを特徴とする電子ファイル管理装置。

【請求項 4】 前記管理手段は、アクセス制限電子ファイルを当該アクセス制限電子ファイルに対するアクセス権限情報に関連づけて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする請求項 3 記載の電子ファイル管理装置。

【請求項 5】 データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、

前記オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアク



セス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、前記オリジナル電子ファイルを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、該アクセス権限情報に基づいて、前記アクセス制限手段にアクセス制限電子ファイルを生成させて出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項 6】 データを受け取って管理する管理手段と、

前記受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、

前記オリジナル電子ファイル、または該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、

前記管理手段は、オリジナル電子ファイルと、当該オリジナル電子ファイルに対するアクセス権限情報と、該アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるよう該オリジナル電子ファイルを暗号化したアクセス制限電子ファイルとを受け取って前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする電子ファイル管理装置。

【請求項 7】 前記アクセス制限電子ファイルは、暗号化された後 I D を付けられ、該 I D に基づいてアクセス権限情報との対応を確認されることを特徴とする請求項 1 から 6 の何れか 1 項に記載の電子ファイル管理装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、例えば技術文書などの電子ファイルを管理し、アクセス権限に応じて活用できるようにする電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

従来より、電子ファイルを管理する電子ファイル管理装置では、格納する電子ファイルに対して予めパスワードを登録させ、ユーザからのアクセス要求を受けると、そのユーザが登録されたパスワードを入力した場合にのみ、そのパスワードに対応する電子ファイルを表示装置や外部記憶装置に出力する。

【0 0 0 3】

また、本出願人により先に出願されている特開 2 0 0 1 - 1 4 2 8 7 4 号公報（特許文献 1）の「文書管理システム」は、電子化された文書を作成して登録し、承認されるとその文書を変換して印刷可能な P D F と印刷不可能な P D F とを作成し、利用権限に応じて閲覧できるファイルを制限するものである。

【0 0 0 4】**【特許文献 1】**

特開 2 0 0 1 - 1 4 2 8 7 4 号公報

【0 0 0 5】**【発明が解決しようとする課題】**

しかしながら、従来の電子ファイル管理装置では、アクセス権限を認められたユーザが電子ファイルを取得した後、アクセス権限を認められていないユーザに取得した電子ファイルを渡すと、アクセス権限を認められていないユーザであってもその電子ファイルにアクセスできてしまうという問題があった。

【0 0 0 6】

また、上述した特許文献 1 の文書管理システムは、電子化された文書を利用権限を認められていないユーザに対しても閲覧のみを許可しつつ印刷を不可能とする好適なものであるが、利用権限を認められているユーザが印刷可能な P D F を読み出した後、他の利用者にその印刷可能な P D F を渡してしまうと、本来印刷可能な P D F へのアクセス権限のない利用者でも P D F を印刷することができてしまっていた。

【0 0 0 7】

本発明はこのような状況に鑑みてなされたものであり、オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアク

セス権限に応じて適切に管理することができる電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を提供することである。

【0 0 0 8】

【課題を解決するための手段】

係る目的を達成するために請求項 1 記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから生成されたアクセス制限電子ファイルとを、当該オリジナル電子ファイルに対するアクセス権限情報に基づいて管理することを特徴とする。

【0 0 0 9】

請求項 2 記載の発明は、請求項 1 記載の発明において、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルと、当該オリジナル電子ファイルから前記アクセス制限手段により生成されたアクセス制限電子ファイルとを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力

する／出力しないことを特徴とする。

【0010】

請求項3記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジナル電子ファイルから前記アクセス制限手段によりアクセス制限電子ファイルが生成されると、該オリジナル電子ファイルを破棄して生成されたアクセス制限電子ファイルを前記格納手段に格納し、アクセス要求を受けると、アクセス制限電子ファイルを前記格納手段から出力することを特徴とする。

【0011】

請求項4記載の発明は、請求項3記載の発明において、管理手段は、アクセス制限電子ファイルを当該アクセス制限電子ファイルに対するアクセス権限情報に関連づけて前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする。

【0012】

請求項5記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、アクセス権限情報を付加されたオリジナル電子ファイルであった場合に、該オリジナル電子ファイルからアクセス制限をかけたアクセス制限電子ファイルを生成するアクセス制限手段と、オリジナル電子ファイル、または／及び該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、前記オリジ

ナル電子ファイルを当該オリジナル電子ファイルに対するアクセス権限情報に関連付けて前記格納手段に格納し、アクセス要求を受けると、該アクセス権限情報に基づいて、前記アクセス制限手段にアクセス制限電子ファイルを生成させて出力する／出力しないことを特徴とする。

【0013】

請求項6記載の発明は、データを受け取って管理する管理手段と、受け取ったデータがオリジナル電子ファイルだけからなるのか、電子ファイルへのアクセス権限を管理するための情報を含むアクセス権限情報とオリジナル電子ファイルとからなるのかを判定する判定手段と、オリジナル電子ファイル、または該オリジナル電子ファイルとアクセス制限電子ファイルとアクセス制限情報とを格納する格納手段と、を備え、管理手段は、オリジナル電子ファイルと、当該オリジナル電子ファイルに対するアクセス権限情報と、該アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるよう該オリジナル電子ファイルを暗号化したアクセス制限電子ファイルとを受け取って前記格納手段に格納し、アクセス要求を受けると、前記アクセス権限情報に基づいて前記オリジナル電子ファイル又は前記アクセス制限電子ファイルを前記格納手段から出力する／出力しないことを特徴とする。

【0014】

請求項7記載の発明は、請求項1から6の何れか一項に記載の発明において、アクセス制限電子ファイルは、暗号化された後IDを付けられ、該IDに基づいてアクセス権限情報との対応を確認されることを特徴とする。

【0015】

【発明の実施の形態】

次に、本発明に係る電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を、図面を用いて詳細に説明する。

まず、本発明の実施形態としての電子ファイル管理装置における、各実施形態に共通する概要について説明する。

【0016】

本発明の実施形態としての電子ファイル管理装置は、装置本体と、ユーザが入

力を行う入力手段と、ユーザに対して各種の情報を表示する表示手段とを備えて構成される。

上記の入力手段は、例えばキーボードやマウスなどであり、表示手段は、例えばディスプレイなどである。

装置本体は、オリジナルのドキュメント（Document；オリジナル電子ファイル）と保護ドキュメント（Protected Document；アクセス制限電子ファイル）との管理を行い、入力手段から操作を行うユーザに認められたアクセス権限に応じて上記の表示手段に出力する。

装置本体からの出力先は上記の表示手段に限定されず、例えばプリンタを装置本体に接続することで、そのプリンタから印字（出力）することもできる。また、ユーザからのアクセス要求がFD（フロッピー（登録商標）ディスク）などのリムーバブルディスクといった情報記録媒体への保存である場合には、その情報記録媒体に保存することとしてよい。

【0017】

次に、本発明の第1の実施形態としての電子ファイル管理装置2について説明する。

この第1の実施形態は、ドキュメント管理プログラム（Document Management Program）21を用いてドキュメント11（オリジナルのドキュメント；オリジナル電子ファイル）、またはドキュメント11とACL（Access Control List；アクセス権限情報）12とを保存した際に、保護ドキュメント13を作成して、基本的にその保護ドキュメント13にのみアクセスさせるモデルである。

【0018】

第1の実施形態における装置本体2aは、ドキュメント11、またはドキュメント11とACL12とを受け取って管理するドキュメント管理プログラム（管理手段）21と、ドキュメント11とACL12とからアクセス制限をかけた保護ドキュメント13を生成するドキュメント保護プログラム（Document Protection Program；アクセス制限手段）22と、電子ファイル（各種ドキュメントやACLなど）を格納するドキュメント管理DB（Document Management DB；格納手段）23と、をHDDなどの記憶部（不図示）に備えてなる。

上記の A C L 1 2 は、ドキュメント 1 1 へのアクセス権限を管理するための情報を含むものである。

【 0 0 1 9 】

この第 1 の実施形態の装置本体 2 a は、物理的には、各種のプログラムやデータなどを記憶する上記した記憶部と、C P U などの主制御部とを備えて構成され、この主制御部が記憶部に格納されたプログラムにより処理を行うことで、この装置本体 2 a は上述した管理手段と、アクセス制限手段と、格納手段として機能する。

すなわち、電子ファイル管理装置 2 は、上記の記憶部に記憶されたドキュメント管理プログラム 2 1 により主制御部が処理を行うことで上記した管理手段として機能し、上記の記憶部に記憶されたドキュメント保護プログラム 2 2 により主制御部が処理を行うことで、上記したアクセス制限手段として機能する。

【 0 0 2 0 】

A C L 1 2 の構成例を図 2 に示す。この図 2 に示す例では、A C L 1 2 は、ユーザ名 (User name) 、アクセスタイプ (Access type) 、許可情報 (Permission) 及び処理要件 (Requirement) をパラメータとして構成される。

すなわち、何らかのアクセス権限を認められたユーザのユーザ名 (User name) に、そのユーザに認められたアクセス権限が、ユーザからの操作命令 (Access type) ごとに関連付けられて構成されている。また、ユーザによる各操作命令ごとに、許可 (Allowed) と拒絶 (Denied) とが定められている。

なお、図 1 、図 2 に示す例では、A C L 1 2 には R e q u i r e m e n t s の項が入っているが、一般的なアクセス制御しかしないのであれば、A C L 1 2 は R e q u i r e m e n t s の項がないものであってよい。

【 0 0 2 1 】

この A C L 1 2 は、ドキュメント 1 1 を作成した作成者や、電子ファイル管理装置 2 の管理者 (管理者権限を持つユーザ) が作成し、そのドキュメント 1 1 に付与しておくこととする。装置本体 2 a は、ドキュメント管理プログラム 2 1 により、入力手段によるユーザからの各操作命令に対し、この A C L 1 2 に基づいて、上述した各種の出力を行う。

【0022】

次に、第1の実施形態にかかる電子ファイル管理装置2における電子ファイル格納時の動作について、図1（a）、図3、図4を参照して説明する。

【0023】

ドキュメント管理プログラム21がドキュメント11とACL12とを受け取って保存する際、ドキュメント管理プログラム21は受け取ったドキュメント11とACL12をドキュメント保護プログラム22に渡して保護ドキュメント13を受け取る。

すなわち、ドキュメント保護プログラム22は、受け取ったACL12に設定されているアクセス権限の制限と同一の制限がドキュメント11にかけられるように、ドキュメント11から保護ドキュメント13を生成する。

【0024】

このドキュメント保護プログラム22による保護ドキュメント13の生成（暗号化）とその復号化にかかるドキュメント保護・印刷システムの構成例を図3に示す。以下の説明では、この保護ドキュメント13の活用（復号化）用途を、プリンタ33により記録紙に印刷することであるとする。

【0025】

この図3に示すドキュメント保護・印刷システムは、電子ファイル管理装置2、印刷用端末31、プリンタ33及びアクセスコントロールサーバ32を有する。

電子ファイル管理装置2と印刷用端末31は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、電子ファイル管理装置2にはドキュメント保護プログラム22が、印刷用端末31にはドキュメント印刷プログラム311がそれぞれ実装されている。

【0026】

ドキュメント保護プログラム22は、ドキュメントファイルに電子ファイル管理装置2の使用者（管理者）の入力操作に応じた印刷要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いて

ドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【0 0 2 7】

ドキュメント印刷プログラム 3 1 1 は、印刷用端末 3 1 の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号化するとともに設定されている印刷要件に応じた印刷処理をプリンタ 3 3 に実行させる処理を行うプログラムである。

【0 0 2 8】

アクセスコントロールサーバ 3 2 は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム 3 1 1 からの要求に応じて A C L 1 2 を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。

アクセスコントロールサーバ 3 2 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース 3 2 1 と、ユーザ各人ごとに設定された印刷要件を含む A C L が登録される A C L データベース 3 2 2 とが接続されている。

【0 0 2 9】

上述のシステムにおいて、ドキュメント 1 1 と A C L 1 2 とを取得したドキュメント保護プログラム 2 2 は、上記の保護ドキュメント 1 3 を生成するに当たって、ドキュメントファイルごとに固有のドキュメント I D（Document ID）を生成し、復号に使用する暗号鍵（Key）と A C L 1 2 とをこれに関連づけてアクセスコントロールサーバ 3 2 へ送信し、登録する。

また、ドキュメント保護プログラム 2 2 は、図 4 に示すように、暗号鍵を用いてドキュメント 1 1 を暗号化し、その暗号化されたドキュメントファイル（暗号化ドキュメント）に対してドキュメント I D を付加して保護ドキュメント 1 3 を生成する。

【0 0 3 0】

こうして保護ドキュメント 1 3 が生成されると、ドキュメント管理プログラム 2 1 は、受け取った保護ドキュメント 1 3 をドキュメント 1 1 及び A C L 1 2 と共にドキュメント管理 D B 2 3 に格納する。こうして、電子ファイル管理装置 2

は、ドキュメント 11 と保護ドキュメント 13 のペア（これをドキュメント・ペア（Document Pair）と呼ぶ）に ACL 12 を付与して（関連付けて）管理する。

【0031】

次に、第 1 の実施形態にかかる電子ファイル管理装置 2 が、管理しているドキュメント・ペアに対してユーザからアクセス要求を受けた時の動作について、図 1（b）、図 3 を参照して説明する。

【0032】

ドキュメント管理プログラム 21 は、ユーザからドキュメント・ペアに対するアクセス要求を受けるとユーザの認証を行う。この認証では、ドキュメント管理プログラム 21 は、ドキュメント・ペアに付与されている ACL 12 を参照して、アクセスしてきたユーザに参照権限がある、すなわち read 権限があると判断すると、保護ドキュメント 13 を返す。すなわち、装置本体 2 a から上述のように表示手段などに出力する。

上記の認証で、アクセスしてきたユーザに参照権限がない、すなわち read 権限が認められていないとドキュメント管理プログラム 21 が判断すると、表示手段にその旨を表示する。

【0033】

この出力された保護ドキュメント 13 の復号化について、上述した図 3 に示すドキュメント保護・印刷システムの例により説明する。

なお、図 3 の例では、ドキュメントファイルを印刷や参照しようとするユーザに対する上述の装置本体 2 a からの出力として、管理者により FD などの情報記録媒体による受け渡しを行う場合と、通信網により印刷用端末 31 へ送信する場合とを示している。

【0034】

ユーザがドキュメントを印刷しようとする場合には、印刷用端末 31 に保護ドキュメント 13 を実装する。例えば、上述のように電子ファイル管理装置 2 から情報記録媒体に出力（記録）された保護ドキュメント 13 を外部記録装置を用いて印刷用端末 31 に読み取らせても良いし、印刷用端末 31 が電子ファイル管理

装置 2 と通信可能である場合には、通信網を介して電子ファイル管理装置 2 から保護ドキュメント 1 3 を印刷用端末 3 1 に出力させるようにしてもよい。

【0 0 3 5】

ユーザが、印刷用端末 3 1 の入力装置を介してドキュメント印刷プログラム 3 1 1 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 3 1 1 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム 3 1 1 は、印刷用端末 3 1 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【0 0 3 6】

ドキュメント印刷プログラム 3 1 1 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 3 2 へ送信して、ユーザ認証を要求する。

【0 0 3 7】

アクセスコントロールサーバ 3 2 は、ドキュメント印刷プログラム 3 1 1 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

ユーザを特定すると、アクセスコントロールサーバ 3 2 は、ACL データベース 3 2 2 を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかといった、アクセス権限の制限の情報を取得する。

ユーザにドキュメントファイル（保護ドキュメント 1 3）を印刷する権限がある場合、アクセスコントロールサーバ 3 2 は、その旨を示す認証情報とともに、保護ドキュメント 1 3 を復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とを印刷用端末 3 1 を介してドキュメント印刷プログラム 3 1 1 に通知する。

【0 0 3 8】

アクセスコントロールサーバ 3 2 から認証情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム 3 1 1 は、暗号鍵を用いて保護ドキュメ

ント 13 を復号化してドキュメント 11 に復元する。

そしてドキュメント印刷プログラム 311 は、印刷要件を満たすようにプリンタ 33 に印刷処理を実行させる。例えば、ドキュメントファイルに BDP が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋を印刷する。

【0039】

以上により、ドキュメントファイルを印刷する際に、管理者がユーザ各人に対して設定した印刷要件、すなわち ACL 12 としてユーザ各人に対して設定したアクセス権限の制限を強制することが可能となる。

【0040】

ここで、ドキュメント 11 から保護ドキュメント 13 を生成する際のドキュメント保護プログラム 22 及びアクセスコントロールサーバ 32 の動作、及び保護ドキュメント 13 をドキュメント 11 に復元して印刷する際のドキュメント印刷プログラム 311 及びアクセスコントロールサーバ 32 の動作についてさらに詳しく説明する。

【0041】

図 4 に、ドキュメント保護プログラム 22 が保護ドキュメント 13 を生成する際の動作を示す。ドキュメント保護プログラム 22 は、電子ファイル管理装置 2 の入力装置における管理者の入力操作によってドキュメントファイルと ACL 12 とを取得すると、ドキュメントファイルの暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム 22 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0042】

さらにドキュメント保護プログラム 22 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメント 13 を生成する。

【0043】

保護ドキュメント 13 を生成した後、ドキュメント保護プログラム 22 は電子ファイル管理装置 2 の通信機能を用いて、暗号鍵と ACL 12 とドキュメント I

Dとをアクセスコントロールサーバ32へ送信し、これらの登録をアクセスコントロールサーバ32に要求する。

【0044】

暗号鍵とACL12とドキュメントIDとをドキュメント保護プログラム22から受け渡されたアクセスコントロールサーバ32は、図5に示すように、これらに関連づけて一つのレコードとしてACLデータベース322に記録保持する。

【0045】

なお、上記の例においてはドキュメントIDの生成や暗号鍵の生成をドキュメント保護プログラム22が行う場合を示したが、これらの処理はアクセスコントロールサーバ32や不図示のサーバなどで行っても良い。

また、電子ファイル管理装置2とアクセスコントロールサーバ32との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0046】

ドキュメント保護プログラム22がアクセスコントロールサーバ32と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (登録商標) RMI (Remote Method Invocation) やSOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ32は、例えばregister(String docId,byte[] key,byte[] acl)のようなメソッドを実装するようにしてもよい。SOAPであれば、HTTPSの上でSOAPプロトコルをやりとりし、RMIであればSSLベースのSocketFactoryを用いてRMIを実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【0047】

次に、ドキュメント印刷プログラム311が保護ドキュメント13を印刷する際の動作について説明する。

図6に、保護ドキュメント13を印刷する際のドキュメント印刷プログラム3

11 及びアクセスコントロールサーバ32の動作の流れを示す。

ドキュメント印刷プログラム21は、印刷用端末31の入力装置におけるユーザの入力操作によって保護ドキュメント13とユーザ名とパスワードとを取得すると、保護ドキュメント13に添付されているドキュメントIDを取得する。

そして、ユーザ名とパスワードとドキュメントIDとアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメント13を印刷しようとするので、“print”となる。）とをアクセスコントロールサーバ32へ送信して、アクセス権限があるか否かのチェックを要求する。

【0048】

アクセスコントロールサーバ32は、ドキュメント印刷プログラム311からユーザ名とパスワードとドキュメントIDとアクセスタイプとを取得すると、ユーザデータベース321に登録されている情報を参照し、ユーザ認証を行う。

換言すると、アクセスコントロールサーバ32は、ユーザデータベース321に登録されている情報を参照し、ドキュメント印刷プログラム311から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース321に組として登録されているか否かを判断する。

【0049】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム311から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース321に登録されていない場合）、アクセスコントロールサーバ32は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」として印刷用端末31へ送信し、ドキュメント印刷プログラム311へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム311へ受け渡すようにしてもよい。

【0050】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ32は、ACLデータベース322に格納されているレコードのうち、ドキュメント印刷プログラム311から取得した情報に含まれるドキュメントIDに関するレコードを読み出す。

【0051】

アクセスコントロールサーバ32は、読み出したレコードに含まれるACL12を取得し、ドキュメント印刷プログラム311から取得したユーザ名及びアクセスタイプに基づいて、ACL12から許可情報および印刷要件を取得する。

換言すると、アクセスコントロールサーバ32は、ユーザ名とアクセスタイプとに基づいて、予めACL12に設定されている許可情報と印刷要件とを取得する。

【0052】

ACL12から取得した許可情報が「許可」である場合、アクセスコントロールサーバ32は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともに印刷用端末31へ送信してドキュメント印刷プログラム311に受け渡す。

一方、ACL12から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ32は、許可情報のみを印刷用端末31へ送信してドキュメント印刷プログラムに受け渡す。

【0053】

アクセスコントロールサーバ32から許可情報を受け渡されたドキュメント印刷プログラム311は、取得した許可情報を参照し、「不許可」である場合には、印刷用端末31の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号化してドキュメントファイルに復元する。

【0054】

また、ドキュメント印刷プログラム311は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PACが指定されていれば機密印刷モードに設定する）、プリンタ33にドキュメントの印刷処理を実行させる。

なお、必要があれば、印刷用端末31の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0 0 5 5】

アクセスコントロールサーバ 3 2 から取得した印刷要件を満足する印刷をプリンタ 3 3 では実行できない場合、換言すると、プリンタ 3 3 が A C L 1 2 に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0 0 5 6】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、A C L データベース 3 2 2 に登録されている A C L 1 2 の内容を電子ファイル管理装置 2 やアクセスコントロールサーバ 3 2 における入力操作によって変更できるようにてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0 0 5 7】

なお、本実施形態を用いる図 3 に示すドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム 3 1 1 に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号化することも可能ではある。この場合は、A C L 1 2 として設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0 0 5 8】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム 2 2 の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

この場合は、ドキュメント印刷プログラム 311 にも同一の秘密鍵を埋め込んでおくことで、管理者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム 311 のみが、保護ドキュメントを復号化して印刷することが可能となる。

【0059】

また、図 3 を用いて上述したドキュメント保護・印刷システムにおいては、ドキュメント印刷プログラム 311 は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム 311 は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat の plug-in としてこの機能を実現することが可能である。

【0060】

なお、この第 1 の実施形態としての電子ファイル管理装置 2 では、上述した図 2 に示す ACL 12 の例には記載していないが、ACL 12 の Access type として例えば Get Original (オリジナル電子ファイルへのアクセス権限) を定義し、その Get Original のアクセス権限を認められているユーザがドキュメント・ペアにアクセスした場合には、ドキュメント管理プログラム 21 は保護ドキュメント 13 を返すのではなく、ドキュメント 11 を返すようにしてもよい。

すなわち、電子ファイル管理装置 2 が Get Original を定義された ACL 12 に基づいてユーザ認証を行い、アクセスしたユーザに Get Original のアクセス権限が認められている場合にはドキュメント 11 を装置本体 2a から上述のように出力するようにしてもよい。

【0061】

また、ACL 12 にオリジナル電子ファイルであるドキュメント 11 へのアクセス権限を定義しなくても、特別なユーザのみ (例えば保存したユーザのみ) がドキュメント 11 へのアクセス権限を認められることとしてもよい。すなわち、ドキュメント管理プログラム 21 が、予め設定された特別なユーザのみにドキュメント 11 へのアクセス権限を認めることとしてもよい。

【0062】

本実施形態によれば、ドキュメント管理プログラム 21 により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置 2 から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【0063】

また、管理者は ACL 12 としてアクセス権限の制限を設定し、ドキュメント 11 と ACL 12 とをドキュメント管理プログラム 21 に渡すよう電子ファイル管理装置 2 を入力手段により操作するだけで、設定したアクセス権限に応じて保護ドキュメント 13 をユーザに渡すよう電子ファイル管理装置に管理させることができる。

すなわち、管理者が ACL 12 としてアクセス権限の制限を一度設定するだけで、電子ファイル管理装置 2 は、表示手段や外部記録装置などへの出力をそのアクセス権限の制限により管理することができる。

【0064】

さらに、上述のようにオリジナル電子ファイルへのアクセス権限を定義することで、電子ファイル管理装置 2 は、上記したアクセス権限の制限による管理をドキュメント 11 と保護ドキュメント 13 とに対して行うことができる。すなわち、電子ファイル管理装置 2 は、ACL 12 として設定されたアクセス権限に応じてドキュメント 11 又は／及び保護ドキュメント 13 を出力するよう管理することができる。

【0065】

なお、本実施形態は、入力されたデータがドキュメント 11 だけからなるものであるのか、ドキュメント 11 と ACL 12 とからなるものであるのかをドキュメント管理プログラム 21 で判定している。データがドキュメント 11 だけからなる場合には、ドキュメント管理プログラム 21 は、そのままドキュメント 11 をドキュメント管理 DB 23 に登録する。このドキュメント 11 に対する要求は、どのようなユーザであっても可能である。

【0066】

次に、本発明の第2の実施形態としての電子ファイル管理装置5について、図7を参照して説明する。

この第2の実施形態は、ドキュメント管理プログラムが、第1の実施形態でドキュメント管理DB23にドキュメント11と保護ドキュメント13（ドキュメント・ペア）をACL12に関連付けて格納していたのに替えて、保護ドキュメント13を格納し、ドキュメント11を破棄するものである。

すなわち、第1の実施形態のようにドキュメント11を残しておく、そのドキュメント11にアクセス可能なユーザがプロテクトされていないドキュメント11を流通させてしまう可能性がある。そのようなことが心配される環境では、この第2の実施形態とすることで保護ドキュメント13を好適に管理することができる。なお、本実施形態においても、ACLの付加されていないドキュメント11は、そのまま格納する。

【0067】

この第2の実施形態の電子ファイル管理装置5における装置本体5aは、物理的な構成は上述した第1の実施形態と同様であり、図7に示すように、ドキュメント管理プログラム51と、ドキュメント保護プログラム22と、ドキュメント管理DB23と、をHDDなどの記憶部（不図示）に備えてなる。

上述した第1の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム22がドキュメント11から保護ドキュメント13を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント13を復号化してプリンタにより印刷する際のシステムや動作も、図3から図6を用いて上述したものと同様であってよい。

【0068】

この第2の実施形態にかかる電子ファイル管理装置5における電子ファイル格納時の動作について、図7（a）を参照して説明する。

ドキュメント管理プログラム51にドキュメント11、またはドキュメント11とACL12を渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム51は、受け取ったデータがドキュメント11だけである

場合、そのままドキュメント管理DB 2 3に登録する。また、ドキュメント 1 1とACL 1 2とを受け取った場合には、ドキュメント保護プログラム 2 2に渡して保護ドキュメント 1 3を受け取る。すなわち、上述のようにドキュメント保護プログラム 2 2に保護ドキュメント 1 3を生成させる。

生成された保護ドキュメント 1 3を受け取ると、ドキュメント管理プログラム 5 1は、受け取った保護ドキュメント 1 3をドキュメント管理DB 2 3に格納し、ドキュメント 1 1とACL 1 2とは破棄する。

【0 0 6 9】

この第2の実施形態にかかる電子ファイル管理装置 5が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図7（b）を参照して説明する。

ドキュメント管理プログラム 5 1はドキュメントに対するアクセス要求を受けると、ドキュメント管理DB 2 3に格納している保護ドキュメント 1 3を返す。すなわち、装置本体 5 aから上述のように表示手段などに出力する。

【0 0 7 0】

本実施形態では、ドキュメント 1 1は破棄され、保護ドキュメント 1 3はユーザによって読み出された後、ACL 1 2に従ってアクセス制御されるため、ドキュメント管理プログラム 5 1でアクセス制御を行う必要はない。

しかし、保護ドキュメント 1 3を取得されると暗号を解読されて内容にアクセスされる可能性もあるため、その可能性を少しでも減らすために、上述した第1の実施形態と同様に、ドキュメント管理プログラム 5 1が保護ドキュメント 1 3をドキュメント管理DB 2 3に格納する際、保護ドキュメント 1 3にACL 1 2を関連付けて格納（ACL 1 2を付与して管理）し、そのACL 1 2に基づいてアクセス制御を行うようにしてもよい。すなわち、上記したドキュメント 1 1を破棄する際に、ドキュメント管理プログラム 5 1はACL 1 2を破棄せず、保護ドキュメント 1 3に関連付けてドキュメント管理DB 2 3に格納することとしてもよい。

このようにアクセス制御を行うことで、ドキュメント管理プログラム 5 1により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制

限) と、ユーザに渡された (装置本体 5 a から出力された) ドキュメント (ポータブルドキュメント) へのアクセス制御とを統一することができる。

【0071】

本実施形態によれば、暗号化されていないドキュメント 1 1 を破棄することにより、管理しているドキュメントをより確実に保護することができる。

【0072】

次に、本発明の第 3 の実施形態としての電子ファイル管理装置 6 について、図 8 を参照して説明する。

この第 3 の実施形態は、ドキュメント管理プログラムが、第 1 の実施形態でドキュメント保護プログラム 2 2 に保護ドキュメント 1 3 を生成させて、ドキュメント管理 DB 2 3 にドキュメント 1 1 と保護ドキュメント 1 3 (ドキュメント・ペア) を ACL 1 2 に関連付けて格納していたのに替えて、ドキュメント 1 1 を ACL 1 2 に関連付けてそのまま格納し、ユーザからアクセス要求を受けた際にドキュメント保護プログラム 2 2 に保護ドキュメント 1 3 を生成させて上述のように出力するものである。

すなわち、第 1 の実施形態のような管理を行う場合、保護ドキュメント 1 3 を保存しておく分だけディスク領域を多く必要とすることになる。そこで、この第 3 の実施形態は、ドキュメントへのアクセスがユーザから要求されたときに動的に保護ドキュメント 1 3 を作成することで、余分なディスク領域を使用せずにすむ好適な管理を行うことができる。なお、本実施形態においてもドキュメント管理プログラム 6 1 は、ACL が付加されていないドキュメント 1 1 を受け取ると、このドキュメントをそのままドキュメント管理 DB 2 3 に登録する。

【0073】

この第 3 の実施形態の電子ファイル管理装置 6 における装置本体 6 a は、物理的な構成は上述した第 1 の実施形態と同様であり、図 8 に示すように、ドキュメント管理プログラム 6 1 と、ドキュメント保護プログラム 2 2 と、ドキュメント管理 DB 2 3 と、を HDD などの記憶部 (不図示) に備えてなる。

上述した第 1 の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム 22 がドキュメント 11 から保護ドキュメント 13 を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント 13 を復号化してプリンタにより印刷する際のシステムや動作も、図 3 から図 6 を用いて上述したものと同様であってよい。

【0074】

この第 3 の実施形態にかかる電子ファイル管理装置 6 における電子ファイル格納時の動作について、図 8 (a) を参照して説明する。

ドキュメント管理プログラム 61 にドキュメント 11 と ACL 12 を渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム 61 は、受け取ったドキュメント 11 に ACL 12 を付与してドキュメント管理 DB 23 に格納する。また、ドキュメント管理プログラム 61 は、受け取ったデータがドキュメント 11 だけであった場合には、このドキュメント 11 をそのままドキュメント管理 DB 23 に登録する。

【0075】

この第 3 の実施形態にかかる電子ファイル管理装置 6 が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図 8 (b) を参照して説明する。

ドキュメント管理プログラム 61 は、ドキュメントに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント 11 に付与されている ACL 12 に基づいてそのユーザにアクセス権限があるかどうか確認する。そのユーザにアクセス権限がある場合、ドキュメント管理プログラム 61 は、ドキュメント管理 DB 23 から指定されたドキュメント 11 と ACL 12 を取り出し、ドキュメント保護プログラム 22 に渡して保護ドキュメント 13 を上述のように生成させて受け取り、その生成された保護ドキュメント 13 をドキュメント管理プログラム 61 への呼び出し側へ返す。すなわち、装置本体 6a から上述のように表示手段などに出力する。

【0076】

なお、この第 3 の実施形態においても、上述した第 1 の実施形態と同様に、ACL 12 の Access type として例えば Get Original (オリ

ジナル電子ファイルへのアクセス権限)を定義し、装置本体6aがユーザ認証を行うことで、GetOriginalのアクセス権限が認められているユーザに対して、保護ドキュメント13ではなく、ドキュメント11を返す(要求に応じて出力する)ようにしてもよい。

【0077】

本実施形態によれば、ドキュメント管理プログラム61により管理・格納されているドキュメントに対するアクセス制御(アクセス権限の制限)と、ユーザに渡された(装置本体6aから出力された)ドキュメント(ポータブルドキュメント)へのアクセス制御とを統一することができる。

【0078】

また、使用するディスク領域を保護ドキュメント13の分だけ小さくすることができるため、ディスク容量が比較的小さい場合であっても好適な管理ができるようになる。

【0079】

次に、本発明の第4の実施形態としての電子ファイル管理装置7について、図9を参照して説明する。

この第4の実施形態は、ドキュメント管理プログラムが、第1の実施形態でドキュメント保護プログラム22に保護ドキュメント13を生成させて、ドキュメント管理DB23にドキュメント11と保護ドキュメント13(ドキュメント・ペア)をACL12に関連付けて格納していたのに替えて、予めドキュメント保護プログラム22に保護ドキュメント13を生成させて保存し、ドキュメント管理DB23にドキュメント11と保護ドキュメント13(ドキュメント・ペア)をACL12に関連付けて格納するものである。

すなわち、電子ファイル管理装置7が内部でドキュメント保護プログラム22を実行するのは、処理のパフォーマンス面から難しくなることも考えられる。そのような場合であっても、あらかじめドキュメント保護プログラム22によってプロテクトした保護ドキュメント13をドキュメント管理プログラム71により保存することで、ドキュメント11と保護ドキュメント13を適切に管理することができるようにするものである。なお、本実施形態においてもドキュメント管

理プログラム 6 1 は、A C L が付加されていないドキュメント 1 1 を受け取ると、このドキュメントをそのままドキュメント管理 D B 2 3 に登録する。

【0 0 8 0】

この第 4 の実施形態の電子ファイル管理装置 7 における装置本体 7 a は、物理的な構成は上述した第 1 の実施形態と同様であり、図 9 に示すように、ドキュメント管理プログラム 7 1 と、ドキュメント保護プログラム 2 2 と、ドキュメント管理 D B 2 3 と、を H D D などの記憶部（不図示）に備えてなる。

上述した第 1 の実施形態と同様のものについては同じ符号とし、説明を省略する。

また、ドキュメント保護プログラム 2 2 がドキュメント 1 1 から保護ドキュメント 1 3 を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント 1 3 を復号化してプリンタにより印刷する際のシステムや動作も、図 3 から図 6 を用いて上述したものと同様であってよい。

【0 0 8 1】

この第 4 の実施形態にかかる電子ファイル管理装置 7 における電子ファイル格納時の動作について、図 9（a）を参照して説明する。

ユーザはまず、ドキュメント保護プログラム 2 2 にドキュメント 1 1 と A C L 1 2 とを渡して保護ドキュメント 1 3 を生成させる。

ドキュメント管理プログラム 7 1 にドキュメント 1 1 と A C L 1 2 と生成された保護ドキュメント 1 3 とを渡し、ユーザが入力手段から格納するよう操作すると、ドキュメント管理プログラム 7 1 は、受け取ったドキュメント 1 1 と保護ドキュメント 1 3（ドキュメント・ペア）をドキュメント管理 D B 2 3 に格納し、受け取った A C L 1 2 を付与して管理する。また、ドキュメント管理プログラム 6 1 は、受け取ったデータがドキュメント 1 1 だけであった場合には、このドキュメント 1 1 をそのままドキュメント管理 D B 2 3 に登録する。

【0 0 8 2】

この第 4 の実施形態にかかる電子ファイル管理装置 7 が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図 9（b）を参照して説明する。

ドキュメント管理プログラム 71 は、ドキュメント・ペアに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント・ペアに付与されている ACL 12 に基づいてアクセス権限があるかどうかを確認する。アクセス権限がある場合には、ドキュメント管理 DB 23 に格納している保護ドキュメント 13 を返す。すなわち、装置本体 7a から上述のように表示手段などに出力する。

【0083】

なお、この第 4 の実施形態においても、上述した第 1 の実施形態と同様に、ACL 12 の Access type として例えば Get Original（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置 7 がユーザ認証を行うことで、Get Original のアクセス権限が認められているユーザに対して、保護ドキュメント 13 ではなく、ドキュメント 11 を返す（要求に応じて出力する）ようにしてもよい。

【0084】

また、この第 4 の実施形態では、ドキュメント保護プログラム 22 は電子ファイル管理装置 7 に替えて、他の装置に実装されていてもよい。この場合、ドキュメント保護プログラム 22 が実装された装置でドキュメント 11 から保護ドキュメント 13 を生成し、その生成を行った装置からネットワークや情報記録媒体などにより装置本体 7a にドキュメント 11 と、保護ドキュメント 13 と、ACL 12 とを渡すこととなる。

【0085】

また、ドキュメント管理プログラム 71 への保存の際にドキュメント 11 と保護ドキュメント 13 を両方渡すのではなく、保護ドキュメント 13 のみを渡してドキュメント 11 を破棄するようにしてもよい。この場合、ユーザからのアクセス要求を受けた際には、上述した第 2 の実施形態と同様の動作となる。

【0086】

本実施形態によれば、ドキュメント管理プログラム 71 により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（装置本体 7a から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【 0 0 8 7 】

また、ドキュメント保護プログラム 2 2 による保護ドキュメント 1 3 の生成を、電子ファイル管理装置 7 における他の重い処理と同時にしないよう行うことができるため、電子ファイル管理装置 7 の処理能力が比較的低い場合であっても保護ドキュメント 1 3 の生成などの処理を適切に行うことができる。

また、ドキュメント保護プログラム 2 2 による保護ドキュメント 1 3 の生成を他の装置で行うことにより、生成などの処理にかかる負担を効果的に分散させることができる。このことにより、電子ファイル管理装置 7 や上記他の装置の処理能力が比較的低い場合であっても、保護ドキュメント 1 3 の生成などの処理を適切に行うことができる。

【 0 0 8 8 】

次に、上述した各実施形態で、印刷用端末 3 に接続されたプリンタ 3 3 から機密印刷にて出力させる場合について説明する。

図 1 0 に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。

【 0 0 8 9 】

まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 3 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 3 1 の動作を図 1 1 に示す。

(1) ドキュメント印刷プログラム 3 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 1 2 に示すように、プリントダイアログを表示させた後に個人識別番号 (Personal Identification Number : P I N) を入力するダイアログを印刷用端末 3 の表示装置に表示させ、ユーザに P I N の入力进行を要求する。

(2) 印刷用端末 3 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 3 1 は、これをプリンタドライバ 3 3 に設定し、印刷を指示する。

プリンタドライバ 3 3 は、ドキュメントから Postscript などの P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印

刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバ 3 3 はさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリンタ 3 3 に送る。

プリンタ 3 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 3 内部の記憶装置 (H D D など) に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 3 3 のオペレーションパネルを介して入力すると、プリンタ 3 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件 (部数、トレイなど) を適用しながら P D L データに従って印刷出力する。

(3) プリンタドライバ 3 3 に P I N が設定できない、すなわち、プリンタ 3 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【0090】

このようにすることで、印刷実行後、プリンタ 3 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 3 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 3 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 3 3 とやりとりを S S L で保護してもよい。

【0091】

また、ドキュメント印刷プログラム 3 1 を Windows (登録商標) Domain のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows (登録商標) Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 3 3 へ送付するようにする。プリンタ 3 3 は、オペレーションパ

ネルでユーザからのパスワード入力を受け、そのユーザIDとパスワードとでWindows（登録商標）Domainのユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（登録商標）Domainに限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒なPIN入力の手間を削減できる。

【0092】

次に、印刷要件としてEBCが設定されている場合のドキュメント印刷プログラム31の動作について説明する。

（1）ドキュメント印刷プログラム21は、EBCが設定されているドキュメントを印刷する際にドキュメントIDを示すバーコード画像データ（又は、二次元コード）のデータを生成する。

（2）ドキュメント印刷プログラム31は、生成したバーコード画像データをスタンプ画像としてプリンタドライバ33にセットし、プリンタ33に印刷を指示する。

（3）プリンタドライバ33にEBCが設定できない、すなわち、プリンタ3がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0093】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメントIDを取得し、そのドキュメントIDを基にアクセスコントロールプログラム32が、ハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【0094】

次に、印刷要件としてBDPが設定されている場合のドキュメント印刷プログラム31の動作について説明する。

（1）ドキュメント印刷プログラム31は、BDPが設定されているドキュメ

ントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro, 2002/08/04 23:47:10）。

（２）ドキュメント印刷プログラム 3 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

（３）ドキュメント印刷プログラム 3 1 は、生成した地紋画像をスタンプとしてプリンタドライバ 3 3 にセットし、プリンタ 3 3 にドキュメントの印刷を指示する。

（４）プリンタドライバ 3 3 に B D P が設定できない場合、すなわちプリンタ 3 3 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【 0 0 9 5 】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、E B C をサポートしていない複写機をしようする場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【 0 0 9 6 】

次に、印刷要件として S L S が設定されている場合のドキュメント印刷プログラム 3 1 の動作について説明する。

（１）ドキュメント印刷プログラム 3 1 は、S L S が設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secret ならば「極秘」のマークなど）を選択する。

（２）選択した画像のデータを、スタンプとしてプリンタドライバ 3 3 にセットし、プリンタ 3 3 に印刷を指示する。

（３）プリンタドライバ 3 3 に S L S をセットできない場合、すなわち、プリンタ 3 3 が S L S をサポートしていない場合には、ラベルスタンプをサポートし

ている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0097】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【0098】

上記の各例は、あくまでも印刷要件の一例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

このように、プリンタ 3 3 がサポートする様々なセキュリティ機能を利用してセキュリティポリシーを設定することによって、プリンタ 3 3 のセキュリティ機能が無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは上述した各実施形態のシステム構成においても同様である。

【0099】

なお、上述した各実施形態は、本発明の好適な実施形態であり、本発明の主旨を逸脱しない範囲内において、種々変形して実施することが可能である。

例えば、上述した各実施形態で用いられる各種ドキュメント（電子ファイル）の内容は、文書に限定されず、例えば画像を含めた文書ファイルや画像ファイルなどであってもよい。

【0100】

また、本発明に係る電子ファイル管理装置が入力手段と表示手段を備えることとしているが、装置本体が上述した動作をできればこの構成に限定されず、例えば、ネットワークを介して接続されたユーザ端末により装置本体がユーザからの入力を受けたり、ネットワークを介して接続された表示装置や外部記録装置に装置本体から出力したりしてもよい。

また、プリンタを装置本体や印刷用端末に接続して出力に用いる場合、ネットワークを介して接続されたものであっても、装置本体や印刷用端末と一体化されたものであってもよい。

【0101】

また、格納手段が複数ある場合、A C L 1 2 などが付与されていることを確認できるのであれば（例えば、上述のように関連付けて格納する、など）、ドキュメント・ペアのそれぞれやA C L 1 2 を異なる格納部に格納してもよい。

【0102】

また、以上に、ドキュメント保護プログラムとしてユーザベース・アクセス制御モデルのものを利用した場合の実施形態について説明したが、アクセス権限を管理するための情報を設定して電子ファイルの管理を行うことができれば本発明はこのものに限定されない。例えば、ポリシーベース・アクセス制御モデルのドキュメント保護プログラムを利用した場合には、A C L ではなくポリシーに従ってアクセスが制御されるだけで基本的には同じ仕組みとして本発明は同様に適用可能である。

【0103】

なお、上述した実施形態では、ドキュメント管理プログラム 2 1 で入力したデータがドキュメント 1 1 だけからなるのか、ドキュメント 1 1 とA C L 1 2 とからなるのかを判定し、ドキュメント 1 1 だけであった場合には、このドキュメント 1 1 をそのままドキュメント管理DB 2 3 に格納している。しかしながら、A C L 1 2 が付加されているか否かに関わらず、すべてのドキュメントの保護ドキュメントを作成するものであってもよい。全てのドキュメントに対して保護ドキュメントを作成しておくことで、オリジナルドキュメントが作成者の許可なく変更される不具合を防止することができる。

【0104】

【発明の効果】

以上のように、本発明によれば、アクセス制限電子ファイルを、アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるように生成し、そのアクセス制限電子ファイルとオリジナル電子ファイルとを上記のアクセス

権限情報に基づいて管理することにより、アクセス権限情報でアクセス権限を認められていないユーザに対して、アクセス制限電子ファイルをたとえ入手したとしてもアクセスできないようにすることができると共に、そのアクセス権限の管理を、管理者（アクセス権限の設定者）がアクセス権限情報を作成するだけで自動的に行うことができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態としての電子ファイル管理装置 2 におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図 2】

印刷要件を含んだ ACL の構造を例示する図である。

【図 3】

保護ドキュメント 13 を印刷に用いるための、保護ドキュメント 13 の生成（暗号化）とその復号化にかかるシステムの構成例を示すブロック図である。

【図 4】

ドキュメント保護プログラム 22 が保護ドキュメント 13 を生成する際の動作を示す図である。

【図 5】

暗号鍵と ACL 12 とドキュメント ID とを関連付けたレコードを例示する図である。

【図 6】

保護ドキュメント 13 を印刷する際のドキュメント印刷プログラム 311 及びアクセスコントロールサーバ 32 の動作の流れを示す図である。

【図 7】

本発明の第 2 の実施形態としての電子ファイル管理装置 5 におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図 8】

本発明の第 3 の実施形態としての電子ファイル管理装置 6 におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図 9】

本発明の第 4 の実施形態としての電子ファイル管理装置 7 におけるプログラムの構成の概要とその動作例を示すブロック図である。

【図 10】

プリンタが備えるセキュリティ機能の一例を示す図である。

【図 11】

PAC が設定されている場合のドキュメント印刷プログラム 31 の動作例を示す図である。

【図 12】

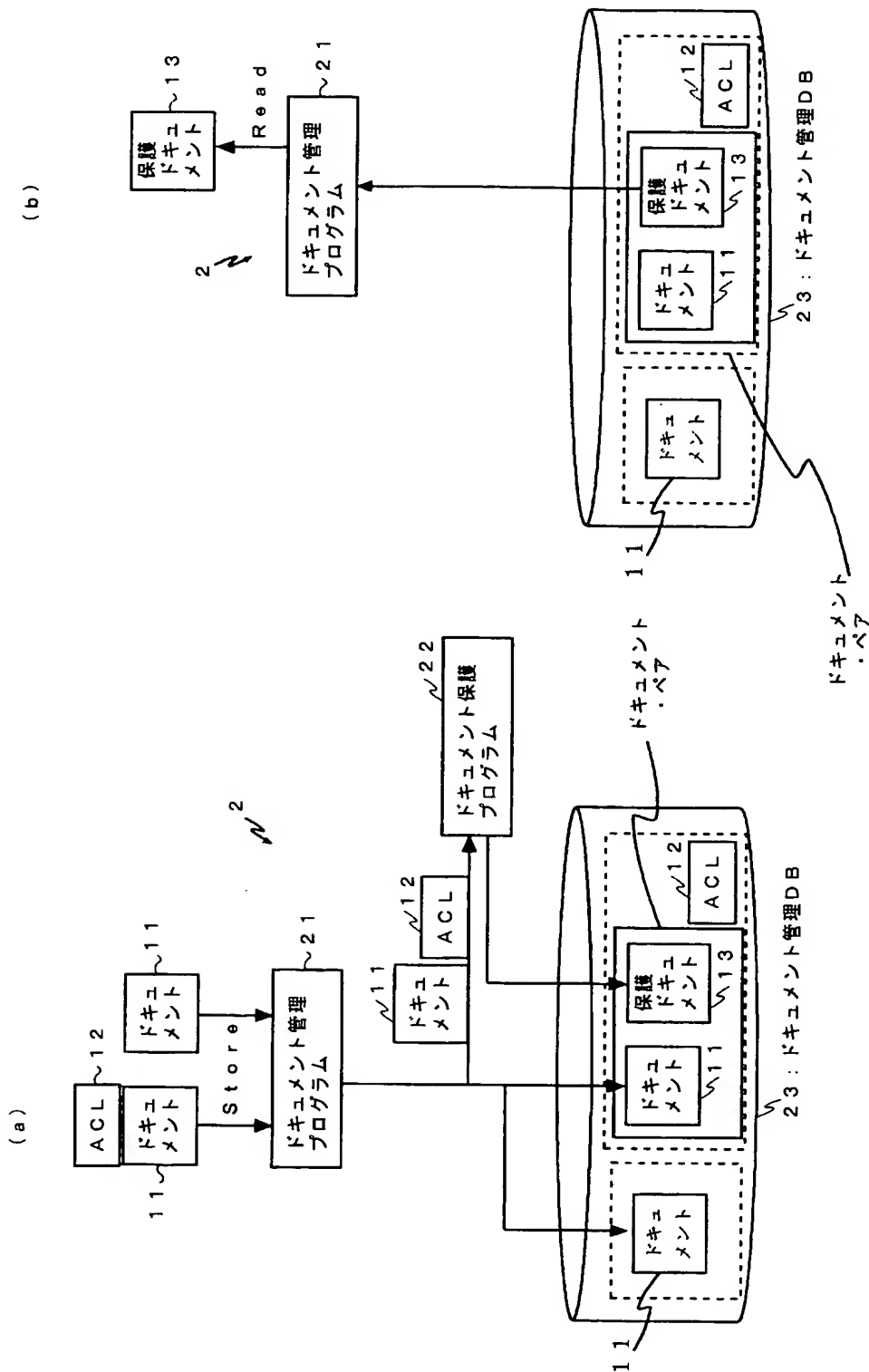
ドキュメント印刷プログラム 31 により PAC が設定されているドキュメントファイルを印刷する際の画面表示例を示す図である。

【符号の説明】

- 11 ドキュメント (オリジナル電子ファイル)
- 12 ACL (アクセス権限情報)
- 13 保護ドキュメント (アクセス制限電子ファイル)
- 2、5、6、7 電子ファイル管理装置
- 2a、5a、6a、7a 装置本体
- 21、51、61、71 ドキュメント管理プログラム (管理手段)
- 22 ドキュメント保護プログラム (アクセス制限手段)
- 23 ドキュメント管理 DB (格納手段)
- 31 印刷用端末
- 311 ドキュメント印刷プログラム
- 32 アクセスコントロールサーバ
- 321 ユーザデータベース
- 322 ACL データベース
- 33 プリンタ

【書類名】 図面

【図1】

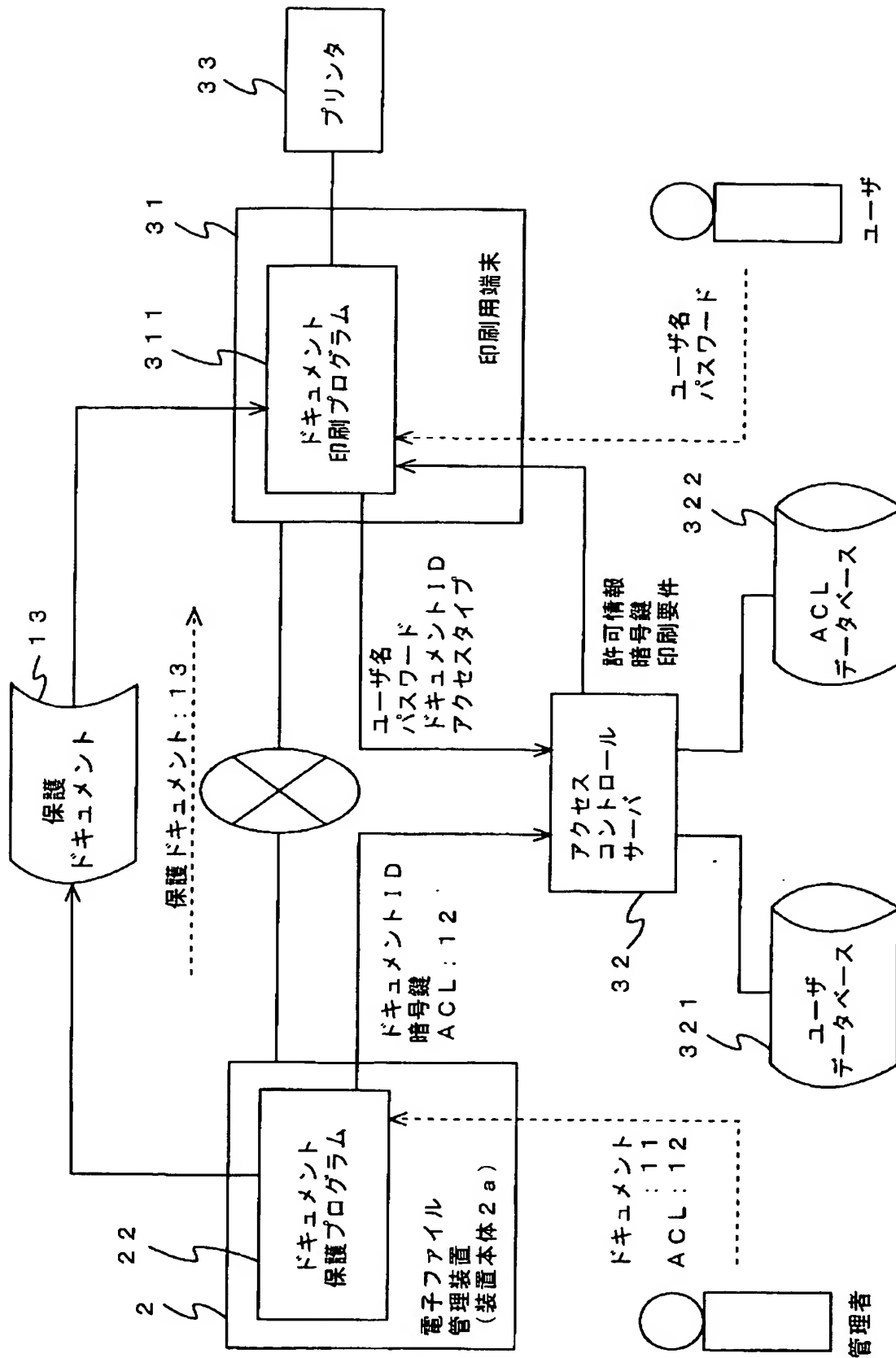


【図 2】

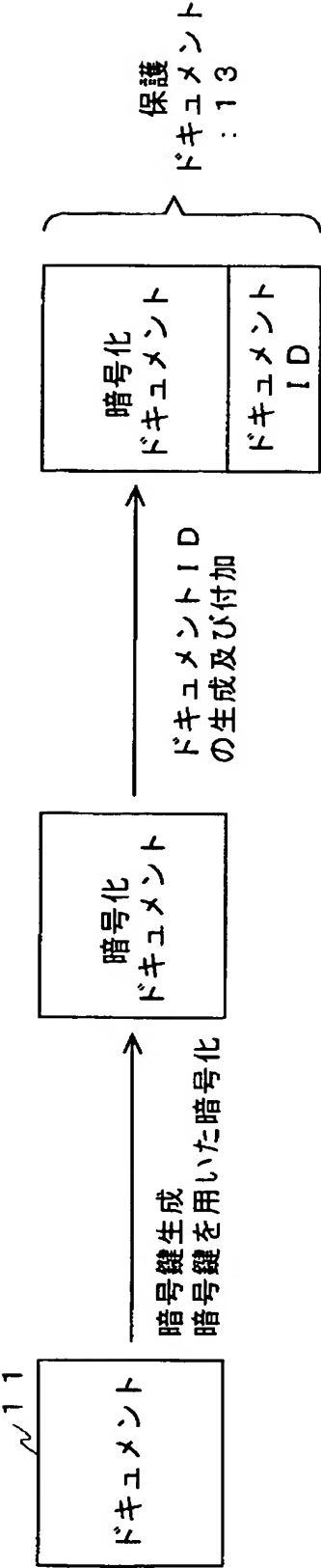
1 2

User name	Access type	Permission	Requirements
RicoH	Read	Allowed	-
	Write	Denied	-
	Print	Allowed	PAC (Private Access)
			BDP (Background Dot Pattern)
			EBC (Embedding Barcode)
	Hardcopy	Allowed	RAD (Record Audit Data)
Taro	Read	Allowed	-
	Write	Denied	-
	Print	Denied	-
	Hardcopy	Denied	-

【図 3】



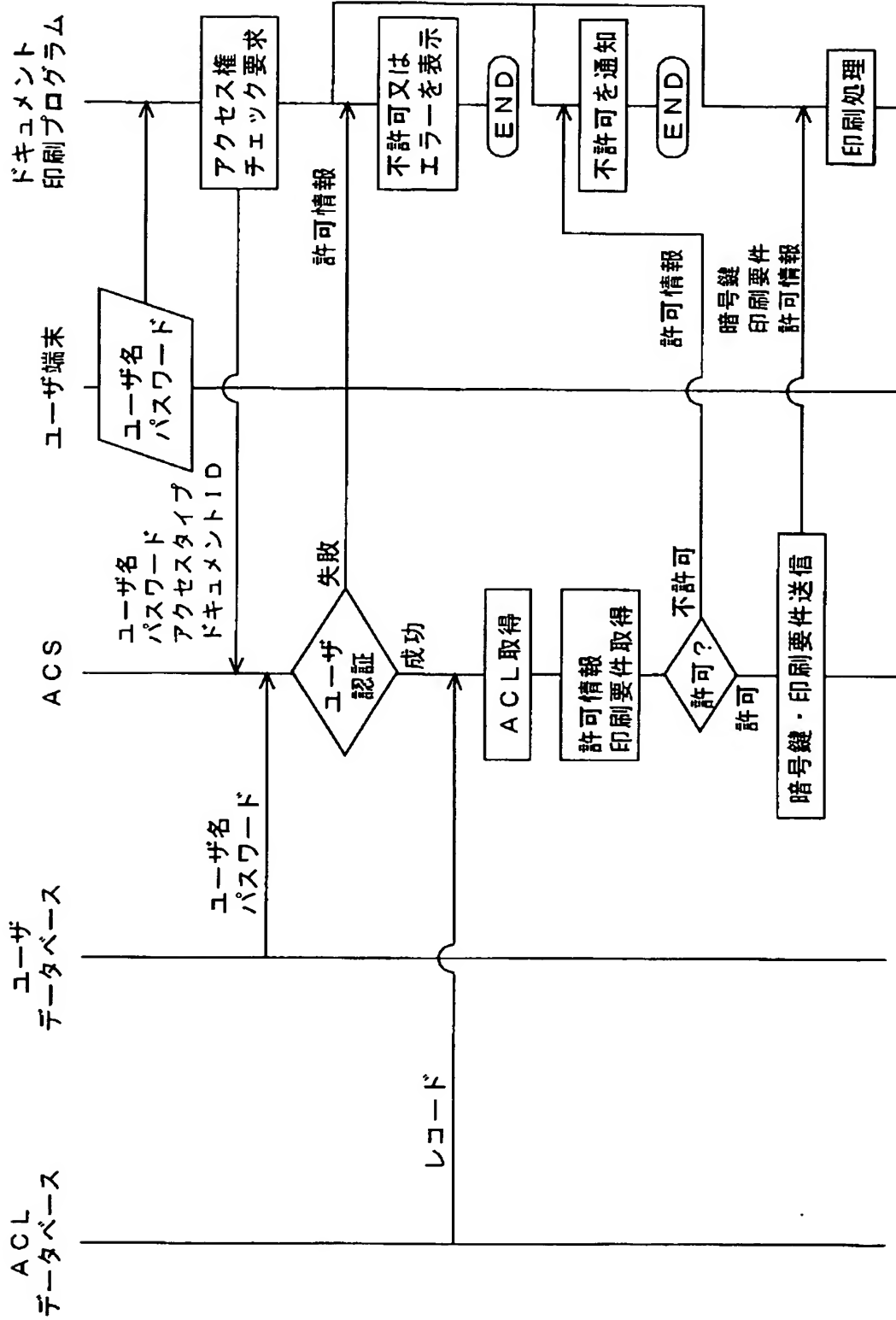
【図 4】



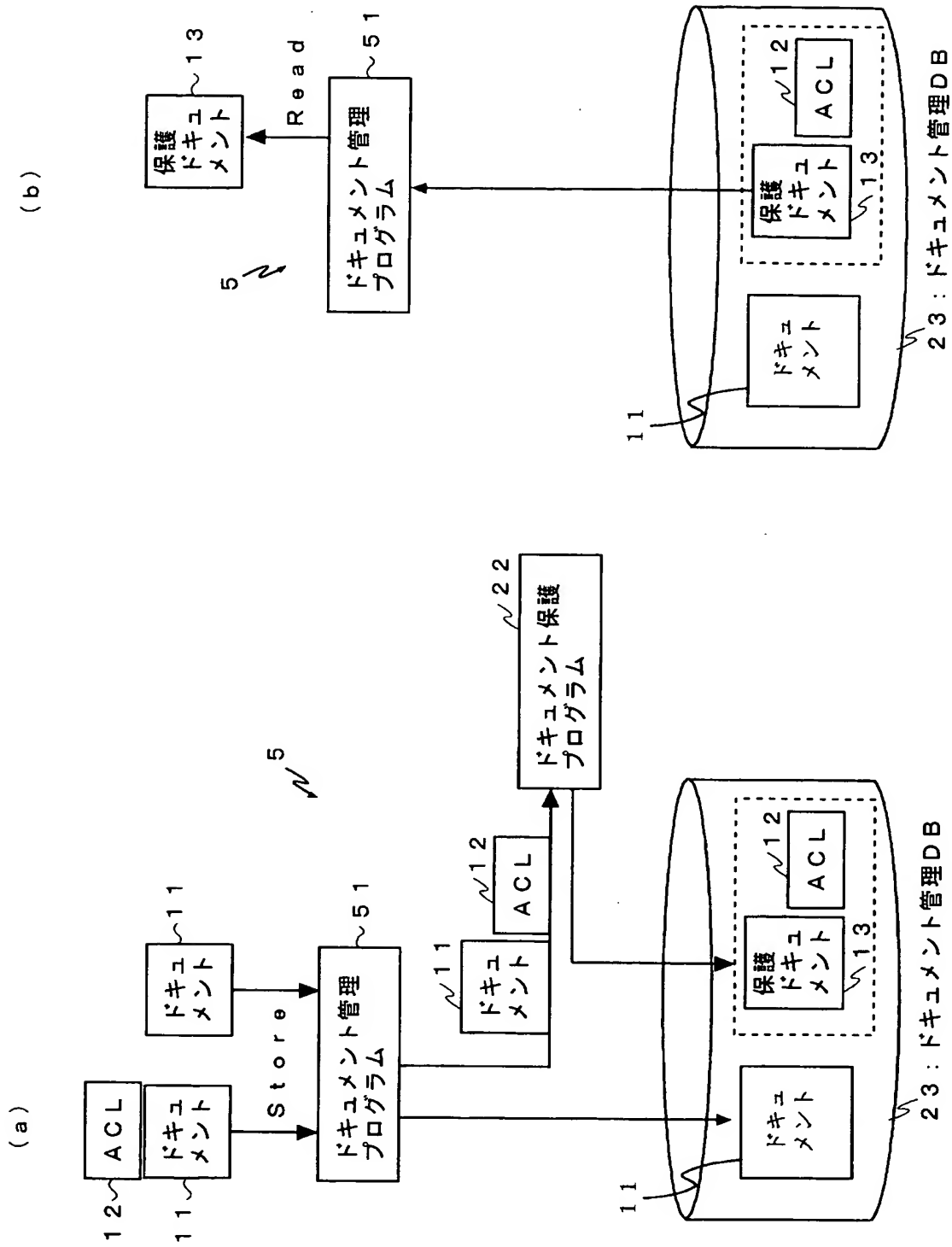
【図 5】

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

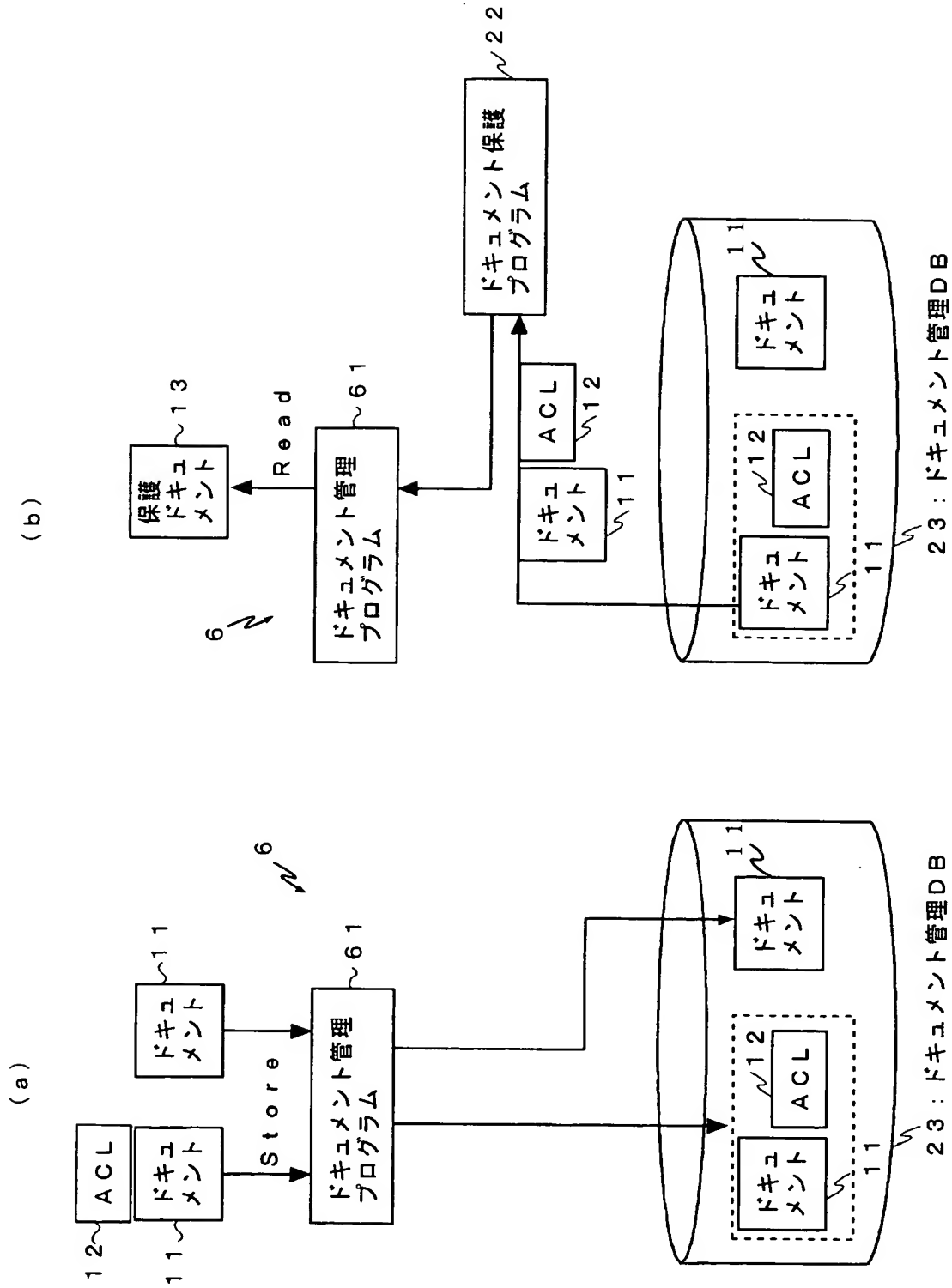
【図 6】



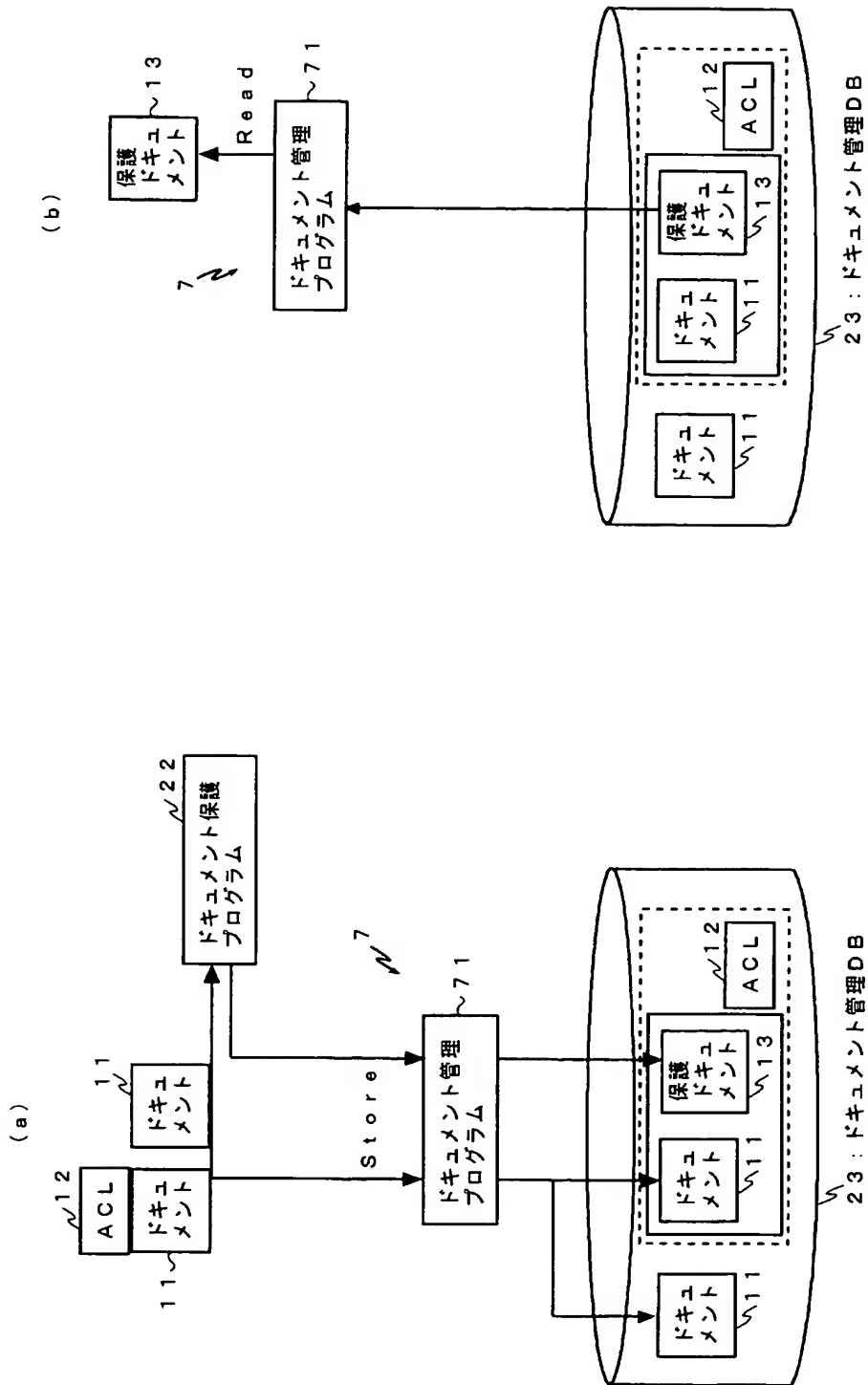
【図 7】



【図 8】



【図 9】

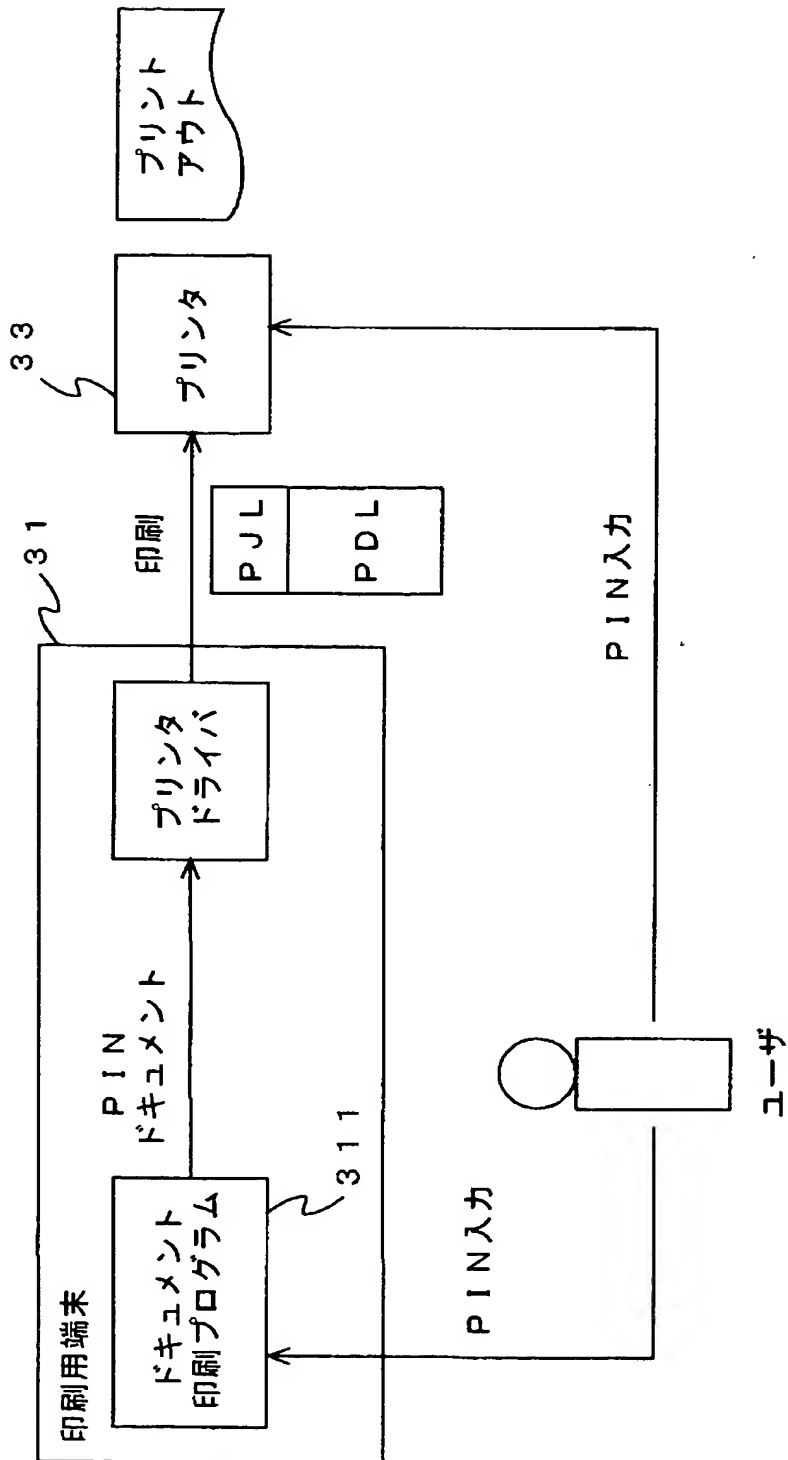


【図 1 0】

プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバに P I N (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでその P I N を入力しなければプリントアウトされない機能。

【図 11】



【図 12】

The diagram illustrates a printer control interface with two main dialog boxes. The top dialog box, titled 'プリントダイアログ' (Print Dialog), contains a 'プリンタ' (Printer) section with a 'プリンタ名' (Printer Name) field and a 'プロパティ' (Properties) button. Below this, the '状態: 通常使うプリンタ: オンライン' (Status: Normally used printer: Online) is shown, followed by a '種類:' (Type:) section with five radio buttons. The '印刷範囲' (Print Range) section offers three options: '全ページ' (All pages) with a selected radio button, '現在のページ' (Current page) with an unselected radio button, and 'ページ範囲' (Page range) with an unselected radio button. The 'ページ範囲' option includes '開始' (Start) and '終了' (End) input fields. The '印刷部数' (Print Count) section features a single input field. The bottom dialog box, titled 'PIN入力ダイアログ' (PIN Input Dialog), contains a message: 'この文書は機密文書ですので機密印刷を行います。暗証番号をセットしてください。' (This document is a confidential document, so confidential printing will be performed. Please set the PIN number.). Below the message is a '暗証番号' (PIN Number) input field, and at the bottom are 'OK' and 'キャンセル' (Cancel) buttons. Arrows indicate the flow from the 'ページ範囲' section of the top dialog to the PIN input dialog.

プリントダイアログ

プリンタ

プリンタ名

プロパティ

状態: 通常使うプリンタ: オンライン

種類:

印刷範囲

全ページ

現在のページ

ページ範囲

開始

終了

印刷部数

PIN入力ダイアログ

この文書は機密文書ですので機密印刷を行います。
暗証番号をセットしてください。

暗証番号

OK

キャンセル

【書類名】 要約書

【要約】

【課題】 オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアクセス権限に応じて適切に管理することができるようにする。

【解決手段】 ドキュメント管理プログラム 21 がドキュメント 11、またはドキュメント 11 と A C L 12 とを受け取って保存する際、ドキュメント管理プログラム 21 は受け取ったドキュメント 11 と A C L 12 をドキュメント保護プログラム 22 に渡し、プロテクトをかけられた保護ドキュメント 13 を受け取る。ドキュメント管理プログラム 21 は、ユーザからドキュメントに対するアクセス要求を受けると、A C L 12 に基づいてユーザの認証を行い、参照権限がある、すなわち r e a d 権限があると判断すると、保護ドキュメント 13 を返す。

【選択図】 図 1



特願 2 0 0 2 - 2 9 9 7 2 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー

2. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー